DEPARTMENT OF THE INTERIOR

MINERALS MANAGEMENT SERVICE MANUAL

TRANSMITTAL SHEET

Release No. 113 October 28, 1986

Subject: Administrative Series
Part 306.7 ADP Security Program
Handbook Conducting an ADP Risk Analysis

EXPLANATION OF MATERIAL TRANSMITTED:

This handbook outlines a standard approach for conducting an ADP Risk Analysis at each sensitive computer installation within the Minerals Management Service.

Assistant Director for Administration

FILING INSTRUCTIONS:

REMOVE:	INSERT:	
None	Handbook:	Release
	306.7-H-1	113
	Conducting an ADP Risk Analysis	

OPR: Information Technology Branch
Information Resources Management Division
Office of Administration

1 #1 40248
(289)

UNITED STATES
DEPARTMENT OF THE INTERIOR

Minerals Management Service

Handbook

CONDUCTING AN ADP RISK ANALYSIS

(MMSM 306.7-H-1)

C-1 40248-288

FOREWORD

This Minerals Management Service (MMS) handbook describes a standard approach for conducting a quantitative ADP risk analysis at each sensitive computer installation within the MMS. It also provides guidance in preparing the required ADP risk analysis report for each. Questions concerning this handbook or the manual chapter on ADP Security, MMSM 306.7, may be directed to the Bureau Information Resources Security Administrator (BIRSA), Information Resources Management Division, Office of Administration. Blank worksheets and other forms used in the various analyses described in this handbook are available from the BIRSA.

Assistant Director for Administration

Date: October 28, 1986

2A3 4D 248 B (288)

TABLE OF CONTENTS

CHAPTER 1. INTRODUCTION

Page

1. Purpose.. 1-1
2. Objective.. 1-1
3. Scope.. 1-1
4. Format... 1-1
5. Certification.. 1-1
6. Definitions.. 1-2

Illustration

Illustration 1 Certification Statement.................. 1-3

Appendix

Appendix 1 Glossary...................................... 1-4

CHAPTER 2. DOCUMENTING THE ADP RISK ANALYSIS REPORT

1. Introductory Chapter..................................... 2-1
   A. Background.. 2-1
   B. Scope... 2-1
   C. References.. 2-1
   D. Definitions... 2-1
   E. Responsibilities...................................... 2-1
2. Narrative Descriptions................................... 2-1

CHAPTER 3. ASSETS ANALYSIS

1. Introduction... 3-1
2. Corequisites... 3-1
3. Asset Identification and Appraisal....................... 3-1

Illustration

Illustration 1 Assets Analysis Worksheet................ 3-3

Appendix

Appendix 1 Examples of Physical Plan Assets............. 3-4

CHAPTER 4. APPLICATIONS ANALYSIS

1. Introduction... 4-1
2. Corequisites... 4-1
3. Key Applications... 4-1
   A. Select Key Applications............................... 4-1
   B. Fill Out Data and Process Security Worksheet......... 4-1

4. Exposures.. 4-1
A. Fill Out Risk Analysis Worksheet..................... 4-1
B. Total Loss Expectancies.............................. 4-2

Illustrations

Illustration 1 Data and Process Security Worksheet....... 4-3
Illustration 2 Risk Analysis Worksheet (Major Threats)... 4-4
Illustration 3 Risk Analysis Worksheet (Minor Threats)... 4-5

CHAPTER 5. THREATS AND VULNERABILITIES ANALYSIS

1. Introduction.. 5-1
2. Corequisites.. 5-1
3. Threats Analysis...................................... 5-1
4. Vulnerability Analysis................................ 5-2

Illustrations

Illustration 1 Threats Analysis Worksheet (Major)........ 5-3
Illustration 2 Threats Analysis Worksheet (Minor)........ 5-4
Illustration 3 Assets/Threats Matrix..................... 5-5

Appendix

Appendix 1 ADP Security--Risk Assessment Questionnaire... 5-6

CHAPTER 6. LOSS EXPOSURE ANALYSIS

1. Introduction.. 6-1
2. Corequisites.. 6-1
3. Annual Loss Exposure.................................. 6-1
A. Threat and Probability Column 6-1
B. Cost Per Occurrence Column 6-2
C. Annual Loss Expectancy (ALE) Column 6-2
D. Total ALE Column 6-2
4. Summaries... 6-2
A. Risk Analysis Summary Worksheet...................... 6-2
B. Rank Threats... 6-3

Illustrations

Illustration 1 Annual Loss Expectancy Worksheet.......... 6-4
Illustration 2 Risk Analysis Summary Worksheet........... 6-5

CHAPTER 7. SAFEGUARD ANALYSIS

1. Introduction.. 7-1
2. Safeguard Categories.................................. 7-1
A. Administrative....................................... 7-1
B. Technical.. 7-2
C. Physical... 7-2

CHAPTER 8. COST BENEFIT ANALYSIS AND SAFEGUARD RECOMMENDATIONS

1. Introduction.. 8-1
2. Corequisites.. 8-1
3. Recommend Appropriate Safeguards.................... 8-1
4. Determine Safeguard Costs........................... 8-1
5. Complete the Net Benefit Worksheet.................. 8-1
   A. Threats/Vulnerabilities.......................... 8-1
   B. Asset.. 8-1
   C. Additional Countermeasures....................... 8-1
   D. Threat Occurrence Rate........................... 8-2
   E. Percentage Reduction in Threat Rate.............. 8-2
   F. Annualized Monetary Loss Expectancy.............. 8-2
   G. Annual Loss Reduction............................ 8-2
   H. Annualized Cost of Countermeasure................ 8-2
   I. Total Net Benefit................................ 8-2
6. Rank Safeguards..................................... 8-2

Illustration

Illustration 1 Worksheet Net Benefit Calculation......... 8-3

CHAPTER 1. INTRODUCTION

1. Purpose. A quantitative risk analysis is required for all sensitive computer installations operated by or on behalf of the MMS in compliance with the Departmental Manual, 306 DM 7.6(D).

2. Objective. The objective of an ADP risk analysis is to assure that the proper balance is maintained between the security protections employed and the probabilities and effect of damages and compromises to people, data, facilities, money, and material.

3. Scope. Each ADP risk analysis, based upon the methodology presented in this handbook, will involve indepth analyses of each sensitive computer installation's assets, applications, threats, vulnerabilities, annual loss exposures, and costs versus benefits of recommended safeguards.

4. Format. The structure of the ADP risk analysis report should follow that of Chapter 2, "Documenting the ADP Risk Analysis Report." Approval for any major variations from the format must first be obtained from the BIRSA. Each report should be typed for insertion in a looseleaf notebook with pages and sections numbered for ease in modification and updating. A title page, certification page, and a table of contents should precede the report.

5. Certification. After management review of the ADP risk analysis report, the installation must be certified for continued operational use. See Certification Statement, Illustration 1. The following personnel should sign and date the final report for the appropriate installation:

A. For the Royalty Management Program:

- Chief, Systems Management Division
- IADPSO or alternate IADPSO

B. For the Offshore Regions:

- Regional Director
- Chief, ADP Section (or similar)
- IADPSO or alternate IADPSO

C. For other installations (i.e., Herndon):

- Division Chief
- Branch Chief
- IADPSO or alternate IADPSO

6. Definitions. See Glossary, Chapter 1, Appendix 1.

2A240248

CERTIFICATION

We have carefully examined the certification findings and recommendations documented in the ________________ ADP risk analysis report, dated ________________. Based on our authority and judgment, and weighing the remaining residual risks against operational requirements, we authorize continued operation of the installation.

________________________ ________________________
Installation ADP Security
Officer

________________________ ________________________
Signature and Date Signature and Date

Glossary

ADP Access Authorization is an administrative determination based upon position sensitivity and the results of an investigation that an individual is trustworthy and may be granted access to automated information resources to the degree required in the performance of assigned duties. Similar to a security clearance.

ADP Installation refers to a "permanent" ADP facility for the support of computer systems (generally, although not necessarily) within close physical proximity, which in turn support a specific group of users.

ADP Risk Analysis is a quantitative examination of the assets and vulnerabilities of a sensitive computer installation based on estimated probabilities and frequencies of varying degrees of exposure to and occurrences of natural disasters/hazards and human and other threats, to establish expected annual losses for the purpose of selecting cost-effective safeguards.

Applications Analysis is a study of the sensitivity and criticality of all the applications processed at the installation in order to determine key applications which support the prime mission of the region or organization.

Assets Analysis is the quantification of the resources which support the computer installation.

Asset Integrity is the replacement value of the asset.

Annual Loss Expectancy (ALE) is the product of the expected loss per harmful event multiplied by the probable number of times per year the harmful event is expected to occur.

Bureau Information Resources Security Administrator (BIRSA) is the individual within the MMS who has responsibility for overall coordination of the MMS ADP Security Program and fulfills the role of the BIRSA, as prescribed by departmental policies. (Specific duties of the BIRSA are detailed in the MMS Manual Chapter on ADP Security, 306.7.9D.)

Computer Applications are the computer programs and procedures required to perform data processing operations.

Computer Installation is the same as "ADP Installation," "Installation," and "Sensitive Computer Installation."

Computer Room(s) refers to the room(s) specially designed to house the computer system(s). A computer installation may have more than one computer room.

Computer System refers to one computer configuration which can be programmed and is used for performing data processing functions. Examples could be VAX 11/780, PDP 11/34, PDP 11/70, Perkin-Elmer 3220, IDS Superbrain, IDS Compustar, and Datapoint 5500.

Continuity of Operations Plan (COOP) is a plan which is developed to ensure ADP support to users during interruptions, emergencies, and disasters. It is maintained by an installation as part of its ADP security program.

Cost/Benefit Analysis is the aggregation of all ALE reductions expected to result from implementation of the countermeasure versus its annualized cost.

Data Confidentiality Loss refers to the dollar loss incurred because of the unauthorized or premature disclosure of sensitive, confidential, or proprietary data.

Data Integrity Loss refers to the dollar loss incurred because of the unintentional, unauthorized, or deliberate destruction or modification of data.

Exposure Zone is equivalent to the boundaries of the installation upon which the ADP risk analysis is being performed.

Fire, Major is a fire which destroys a major piece of equipment or severely impacts computer operations. For example, the complete burnout of a computer mainframe.

Fire, Minor is a small fire confined to one piece of equipment or a small area. For example, a fire in a tape drive.

Installation is the same as "ADP Installation," "Computer Installation," and "Sensitive Computer Installation."

Installation ADP Security Officer (IADPSO) is designated for each installation and ensures that the installation continuously meets all security requirements necessary to protect the installation. (Specific duties of the IADPSO are detailed in the MMS Manual Chapter on ADP Security, 306.7.9D.)

Loss Expectancy refers to a specific dollar loss incurred in terms of operational reliability, data confidentiality, data integrity, or the realization of a harmful event.

Loss Exposure Analysis is the process of quantitatively estimating the monetary loss caused by a threat acting upon the assets and applications vulnerable to that threat.

Major Threat is an installation-specific determination of the magnitude of an event which threatens all of the facility's resources.

Minor Threat is an installation-specific determination of the magnitude of an event which threatens portions of the facility's resources.

Operational Reliability Loss refers to the dollar loss incurred as the result of undependable, inadequate, delayed, or unavailable processing.

Physical Plant is the same as "Exposure Zone."

Proprietary Data is data (owned by the Government or some other organization) which if disclosed prematurely or without authorization, would cause serious legal and financial complications.

Remote Terminal is any terminal (e.g., microcomputer or communicating word processor) which is used to remotely access any computer system via telecommunications, as opposed to a terminal with hardwired communications connections.

Sensitive Application is any computer application which requires a degree of protection because it processes sensitive data or because of the risk and magnitude of loss or harm that could result from improper operation or deliberate manipulation of the application.

Sensitive Computer Installation is any computer installation where sensitive applications are processed or which requires a degree of protection due to the magnitude of loss or harm which could result from misuse or loss of the installation. The term includes ALL computer installations for the purposes of this handbook.

Sensitive Data includes any data which requires a degree of protection due to the risk and magnitude of loss or harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the data. Included is data affecting the mission of the MMS or the Department of the Interior. Also included are personal data requiring protection in accordance with the Privacy Act; data contained in automated decisionmaking applications; financial data which could result in loss to the Government if not fully protected; proprietary data warranting special protective measures; and any other data the special protection of which is determined to be in the best interest of the Government.

Threats are any situations or conditions which could adversely affect an installation or its operations, or the integrity, reliability, or confidentiality of its data.

Threats and Vulnerabilities Analysis is the process of identifying the various threats to and vulnerabilities of the computer installation in terms of potential loss.

Total Loss Expectancy is the sum of the data integrity, data confidentiality, and operational reliability dollar losses incurred.

Vulnerabilities are weaknesses.

CHAPTER 2. DOCUMENTING THE ADP RISK ANALYSIS REPORT

1. Introductory Chapter. The following is an outline of the components to be documented in Chapter 1 (Introduction) of the report upon the completion of the installation's ADP risk analysis.

A. Background. Provide a complete overview discussion, including the rationale and justification for performing the risk analysis of the installation at the given time.

B. Scope. Establish the scope of the risk analysis by defining the bounds of the installation involved.

C. References. Reference any sources of information used in the study. Include the following:

(1) Departmental Manual, 306 DM 7, ADP Security Program.

(2) ADP Standards Handbook, 306 DM 2, ADP Security Program.

(3) MMSM 306.7, ADP Security.

(4) MMSM 306.7-H-1, Handbook, Conducting an ADP Risk Analysis.

(5) FIPS PUB 31, Guidelines for Automatic Data Processing Physical Security and Risk Management.

(6) FIPS PUB 65, Guidelines for Automatic Data Processing Risk Analysis.

D. Definitions. Define the key terms used in the risk analysis. These may be expanded from the Glossary in this handbook.

E. Responsibilities.

(1) The IADPSO has responsibility for the preparation and maintenance of this document as detailed in MMSM 306.7.9D. Reference to this responsibility should be incorporated here.

(2) List the names and titles of all individuals who helped develop the report if different from (1). Include all individuals interviewed.

2. Narrative Descriptions. Chapters 2-7 of the risk analysis report will consist of narrative descriptions summarizing the documentation of each aspect of the completed study. Specific aspects of the study are discussed in Chapters 3 through 8 of this handbook. Reference the completed worksheets as appropriate in each chapter and attach them as appendices to the report.

CHAPTER 3. ASSETS ANALYSIS

1. Introduction. In order to determine expected losses in the event of probable threats occurring, it is necessary to identify the installation's major assets and their associated replacement costs and/or lease/maintenance charges. The results of this analysis will be documented in the Assets Analysis Worksheet (Illustration 1) and will be used later in the study in determining ALE's.

2. Corequisites.

A. The Assets Analysis Worksheet.

B. Interviews with appropriate individuals who can identify those assets which should be included in the study and who can supply replacement values and/or lease/maintenance charges.

C. Current ADP hardware inventory listing. This should be appended with the completed worksheets.

3. Asset Identification and Appraisal. For this task use the Assets Analysis Worksheet.

A. Determine the Exposure Zone or the Physical Plant upon which the ADP risk analysis is to be conducted. This should correlate with the bounds of the installation as discussed in Chapter 2.1B of this handbook.

B. List owned assets and value (replacement cost) and leased assets with lease/maintenance charges as applicable for each of the following components on the Assets Analysis Worksheet. Refer to Illustration 1 of this chapter for a completed example. Exact dollar figures are not necessary as a rounded figure will not affect the outcome of the analysis.

(1) Physical Plant. List the major assets and the replacement costs or lease/maintenance fees of the Physical Plant. Examples of physical plant assets are provided in Appendix 1.

(2) Hardware. Total the owned and leased assets of all equipment used in association with the installation's data processing.

(3) Personnel. The value of personnel assets is based upon need for and availability of replacement and any associated training. In the event any installation personnel are "lost," the costs for both replacement and training will generally be nominal because of the number of highly technical individuals available in the Federal work force. If this is not applicable to the installation in question, however, determine the value of personnel assets and include this information on the worksheet.

(4) New Site Costs. Determine the cost of rebuilding those rooms essential in the operation of the installation (i.e., the computer room with raised floor, ramps, special drains, and, user rooms, etc.).

(5) Supplies. List the replacement costs of all computer related supplies normally stocked at the installation.

(6) Total Assets. This is the total of the replacement costs and lease/maintenance costs of the assets identified in 3B(1) through (5).

ASSETS ANALYSIS WORKSHEET

<u>Alaska OCS Region</u>

<u>Assets</u>

1. Physical Plant	
UPS	$ 50,000
Halon	100,000
A/C	100,000
Alarm System	80,000
Furniture and Costs	30,000
Cabling (60 feet x $150/ft)	9,000
Emergency Lighting	10,000
Safe	5,000
	$ 384,000
2. Hardware	$1,000,000
3. Personnel	$ 0
4. New Site Costs	$ 150,000
5. Supplies	
Disk Packs ($800/pk x 16 packs)	$ 12,800
Tapes ($500/tape x 20 tapes)	10,000
Paper	12,000
	$ 34,800
6. Total Assets	$1,568,800

Examples of Physical Plant Assets

1. Electrical systems such as:

(a) an uninterruptible power supply system (UPS), or

(b) a power sifter or surge protector.

2. Fire alarm/detection/extinguishing systems such as:

(a) area fire extinguishing systems - Halon, sprinkler or other,

(b) smoke detectors,

(c) any related and/or integrated fire alarm/detection systems, and

(d) portable extinguishers.

3. Environmental systems such as:

(a) air conditioning systems,

(b) humidifiers,

(c) moisture detection systems, and/or

(e) emergency lighting.

4. Furniture.

5. Equipment cables.

6. Security systems such as:

(a) card key systems,

(b) intrusion detection systems, and

(c) other alarm systems.

7. Communications equipment.

CHAPTER 4. APPLICATIONS ANALYSIS

1. Introduction. This overview of application systems processed at the installation will be documented in the Data and Process Security Worksheet (Illustration 1) and will also be used later in the study in determining ALE's (see Chapter 6 of this handbook).

2. Corequisites.

A. The Data and Process Security Worksheet.

B. The Risk Analysis Worksheet (Illustrations 2 and 3).

C. Interviews with users of each application system or other knowledgable persons who can provide the following general information for each key application identified.

(1) The sensitivity and/or criticality of each.

(2) All methods of transmission used.

(3) Any security required.

(4) How many staff-hours it would take to rebuild the system from the last backup.

(5) How much money might be involved in the event of a lawsuit because of unauthorized disclosure of sensitive data.

(6) How many staff-hours it would take to provide an acceptable continuity of service to users in the event the computer used to process the application were unavailable.

3. Key Applications. For this task use the Data and Process Security Worksheet.

A. Select Key Applications. Identify all the applications processed at the installation. Define key applications by determining which are essential to the mission of the region or the MMS, involve proprietary or other sensitive information, and are time critical.

B. Fill Out Data and Process Security Worksheet. Include only the key applications selected in 3A of this chapter.

4. Exposures. For this task use the Risk Analysis Worksheets.

A. Fill Out Risk Analysis Worksheets. The Loss Expectancy and Total Loss Expectancy must be calculated for each key application on each computer system for both major and minor threats.

Completed examples are provided in Illustrations 2 and 3 of this chapter. Instructions are as follows:

(1) Use only the key applications selected in 3A of this chapter.

(2) Define the impact of major and minor threats on the installation in terms of the most and the least amount of data that could be lost in the event of any threat. Refer to the glossary as necessary. Do not be concerned with types of threats at this stage.

(3) Calculate the losses incurred for each of the following based upon the definitions provided in the glossary and any installation-specific conditions.

(a) Data Integrity. This must be based upon the installation's major and minor threat assumptions. The data integrity is then calculated by determining how many staff-hours at a determined wage rate it would take to rebuild the application and/or reinput the data from the last backup. A standard of $20/hour for a professional hourly wage is generally accepted.

(b) Data Confidentiality. This is determined by considering how much money might be involved in the event of any legal proceedings or other consequences of the unauthorized or premature disclosure of data.

(c) Operational Reliability. This is calculated by determining how many man-hours at a determined wage rate it would take to provide an acceptable level of service to users in the event the computer used to process the application were unavailable.

B. Total Loss Expectancies. Summarize the Total Loss Expectancies for major and minor threats for each application in a table for later use. An example of the Total Loss Expectancies for key applications at the Alaska OCS Region Computer Installation is provided below.

TOTAL LOSS EXPECTANCIES

Key Applications	Major Threats	Minor Threats
GNG	$128,400	$3,336
Post-sale	6,720	3,520
Montcar	1,920	800
Presto	1,920	800
OIS	178,000	2,000
CLASS	198,000	8,640
OCSIS	81,840	2,560

MINERALS MANAGEMENT SERVICE
DATA AND PROCESS SECURITY WORKSHEET

Organization: MMS

Date: 12-4-85

ADP Installation: Alaska OCS Region

System: Perkin-Elmer (PE)

Application/File/ Process Name	Sensitivity/ Criticality	Method of Transmission	Security Required
GNG	Sensitive	Mail for tape	Maps and original tapes in vaults
(Mapping System)	Time Critical		
	for Lease		
	Sales		
Post Sale	Sensitive		
	Proprietary	PC input/floppy disks	
		Telecommunications	
	Time critical	Reports to headquarters	
	day of sale	PE to Amdahl	

MINERALS MANAGEMENT SERVICE
RISK ANALYSIS WORKSHEET
MAJOR THREATS

Organization: MMS
ADP Installation: Alaska OCS Region
Date: 11-5-85

Threat Type:

Major

System/Application	Loss Expectancy			
	Data Integrity	Data Confidentiality	Operational Reliability	Total Loss Expectancy
GNG	$520/tape		12 people	
	x50 tapes	$1 million	2 weeks	
			$20/hour	
	$26,000		$38,400	$ 64,400
	2 people programming			
	1 month $20/hour			
	$ 6,400			$ 6,400
	3 people digitizing			
	2 months $20/hour			
	$19,200			$ 19,200
	4 people systems support			
	3 months $20/hour			
	$38,400			$ 38,400
TOTAL	$90,000		$38,400	$128,400

MINERALS MANAGEMENT SERVICE
RISK ANALYSIS WORKSHEET
MINOR THREATS

Organization: MMS
ADP Installation: Alaska OCS Region
Date: 12-5-85

Threat Type:
Minor

System/Application	Loss Expectancy			
	Data Integrity	Data Confidentiality	Operational Reliability	Total Loss Expectancy
GNG	9 people		12 people	
(Mapping System)	1 day	$1 million	1 day	
	x $20/hour		x $20/hour	
Total	$1,440		$1,920	$3,360

CHAPTER 5. THREATS AND VULNERABILITIES ANALYSIS

1. Introduction. The identification of specific threats to and vulnerabilities of the ADP installation are prerequisite in quantifying probable losses. This in turn will serve as the basis for recommending cost-effective countermeasures (see Chapter 8 of this handbook).

2. Corequisites.

A. ADP Security--Risk Assessment Questionnaire (Appendix 1).

B. Threats Analysis Worksheets (Illustrations 1 and 2).

C. Assets/Threats Matrix (Illustration 3).

D. Interviews with users, regional personnel, and/or other regional sources to determine major and minor threats and their frequency of occurrence. Frequencies may be based upon experience and/or documented studies such as those in FIPS PUB 31. Other good sources of information include insurance companies, local police and fire authorities, the Federal Bureau of Investigation, the Inspector General, the local weather bureau, the Central Intelligence Agency, and the building engineer or facilities person.

3. Threats Analysis.

A. For this task, first fill out the ADP Security--Risk Assessment Questionnaire.

(1) Identify all possible threats to the assets and key applications. Include any of the following should they apply:

(a) Physical Damage such as fire, natural hazards, water damage, and accidental and intentional damage.

(b) Delayed Processing such as hardware or software failure because of power outages or transients, telecommunications outages, user input errors, air conditioning failure, and operator errors.

(c) Fraud.

(d) Improper Disclosure such as unauthorized or premature disclosure of data.

(e) Physical Theft.

(2) For this task, use the Assets/Threats Matrix.

(a) Fill out the row labeled "ASSETS" with all assets identified on the Assets Analysis Worksheet.

(b) Fill out the column labeled "THREATS" with all threats identified in 3A(1) of this chapter.

(c) Place an "x" or other mark in each box in which the asset would be affected by the corresponding threat.

B. For this task, use the Threats Analysis Worksheets. Completed examples of these worksheets are provided in Illustrations 1 and 2 of this chapter.

(1) Separate threats into major and minor threats, based on installation-specific conditions (see Chapter 4.4A(3)).

(2) List major threats and rates of occurrence on the appropriate Threats Analysis Worksheet. For example, at the Alaska OCS Region's computer installation, a major fire was expected at the rate of once every 30 years. Do the same for minor threats.

4. Vulnerability Analysis.

A. For this task, refer to the completed ADP Security--Risk Assessment Questionnaire.

(1) Identify all possible weaknesses of the assets and applications to the threats previously identified and categorize them into the following:

(a) Administrative Weaknesses. These relate to the overall management policies, standards, procedures, and guidelines.

(b) Technical Weaknesses. These relate to all aspects of the hardware and software systems and their usage.

(c) Physical Weaknesses. These relate to environmental systems, physical access controls, etc.

THREATS ANALYSIS WORKSHEET
MAJOR

Alaska OCS Region

Major Threats

Frequency	Type
1/30 years	Major Fire
1/20 years	Natural Hazard (Earthquake, Wind)
1/10 years	Internal Water Damage
1/10 years	Intentional Release/Disclosure of Data

THREATS ANALYSIS WORKSHEET
MINOR

Alaska OCS Region

Minor Threats

Frequency	Type
1/3 years	A/C Failure
1/3 months	Hardware Failure, PE
1/year	Software Failure
1/10 years	Unauthorized Physical Access
1/year	Accidental damage to data, hardware, software (spilling coffee, etc.)
1/20 years	Unauthorized access to data
1/year	Intentional Damage (Bomb threat, etc.)

Note: A minor threat occurrence would disrupt the system for 1 day.

ASSETS/THREATS MATRIX

ASSETS THREATS	Physical Plant	Elect. Power System	A/C Sys	Mag. Storage Devices	CPU	Local I/O Dev.	Comm Eqpt	Remote I/O Dev.	OS	Document & Software		Sens Data	Non-Sens Data	Comp Opr.	Sys. Prog Adm.	Appl Prog	Security Officer
										Vendor	Appl						
Computer Room Fire	●	●	●	●	●	●	●	●	●	●		●	●	●			●
Building Fire	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Mother Nature (Major)	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Intentional Damage to Hardware, Software, Data, Physical Plant	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Internal Water Damage	●	●	●	●	●	●	●	●	●	●	●	●	●				
Power Failure		●	●	●	●	●	●	●				●	●	●			
AC Failure			●														
Communication Failure							●	●									
Hardware Failure				●	●	●	●	●				●	●	●	●		
Software Failure									●	●	●	●	●	●	●	●	
Data Entry Failure									●	●	●	●	●			●	
Improper Handling of Sensitive Data												●		●	●	●	●
Accidental Damage to Hardware, Software Data, Physical Plan	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Fire (Minor)	●	●	●	●	●	●	●	●	●	●	●	●	●				●

Minerals Management Service
ADP SECURITY--Risk Assessment Questionnaire

Name of Installation ____________

Date ____________

CONTROLS AND PROCEDURES	Yes	*Risk Is Acceptable	*Corrective Action
1. Has the responsibility for the protection of each and every ADP resource (computer system, data, programs, etc.) been explicitly assigned?			
2. Are procedures in place to inform employees what resources they are expected to protect and from what hazards, what variances they are to note, and what corrective action they are to take?			
3. Are procedures in place to ensure the timely and complete separation of terminated employees?			
4. Is there a policy consistent with generally accepted practice about who may access and update data?			
5. Where indicated by the sensitivity of the resource and size of user population, is the policy enforced by the system?			
6. Is each individual user of system uniquely identified?			

* These 3 response columns are mutually exclusive. Columns 2 and 3 are to be completed only if column 1 is not.

	Yes	*Risk Is Acceptable	*Corrective Action
7. Is there a procedure (e.g., password, magnetic-stripe card) to authenticate the identity of the individual user of the system?			
8. Are users restricted to only those resources (e.g., data sets, records or segments, fields, transactions, etc.) required for their jobs?			
9. Are the access rules up to date?			
10. Is access to sensitive facilities (or zones within them) limited to those people who work in that facility on that shift and authorized, escorted visitors?			
11. Are all employees informed of their security roles?			
12. Do all resources receive at least the minimum protection appropriate to their sensitivity?			
FIRE PRECAUTIONS			
1. Do the computer room operators know exactly what to do when the different types of fire emergencies occur?			
2. Are clear and adequate fire instructions posted?			
3. Are the fire alarm pull boxes and emergency power switches clearly visible, identified, and unobstructed?			

* These 3 response columns are mutually exclusive. Columns 2 and 3 are to be completed only if column 1 is not.

	Yes	*Risk Is Acceptable	*Corrective Action
4. Are the machine operators familiar with the different levels of power-off procedures?	____	________	________
5. Are the operators trained periodically in fire fighting?	____	________	________
6. Does the machine room have automatic extinguishers of the following types:			
(a) Sprinkler?	____	________	________
(b) Carbon dioxide flooding?	____	________	________
(c) Halon flooding?	____	________	________
7. Does the computer room have portable extinquishers in suitable locations?	____	________	________
Are these extinquishers immediately accessible and vividly marked?	____	________	________
8. If carbon dioxide or halon flooding is used, are the personnel safety precautions adequate?	____	________	________
9. Is the water supply adequate?	____	________	________
10. Is the fire detection system adequate:			
(a) In the ceiling?	____	________	________
(b) In the air ducts?	____	________	________
(c) Under the raised floor?	____	________	________
11. Is the fire detection system tested frequently?	____	________	________
12. Are the extinquishers checked frequently?	____	________	________

* These 3 response columns are mutually exclusive. Columns 2 and 3 are to be completed only if column 1 is not.

	Yes	*Risk Is Acceptable	*Corrective Action
13. Does the emergency power shutdown switch power off the air conditioning?			
14. Can emergency crews gain access to the installation without delay?			
15. Is smoking prohibited in the computer area?			
16. Are the following combustible materials avoided in the computer area:			
(a) combustible curtains and rags?			
(b) flammable cleaning fluids?			
(c) excess paper and supplies?			
17. Are the floors and ceiling noncombustible?			
18. Is the space under the raised floor cleaned regularly?			
19. Is the cleanliness of the computer area adequate?			
20. Are areas adjoining the computer area suitably protected from fire?			
21. Is there emergency (battery operated) lighting in the computer room?			
22. Does the fire alarm sound:			
(a) outside the computer area?			
(b) at a guard station?			

* These 3 response columns are mutually exclusive. Columns 2 and 3 are to be completed only if column 1 is not.

	Yes	*Risk Is Acceptable	*Corrective Action
(c) at a headquarters location?			
(d) at the local fire station?			
23. Is there 24-hour coverage of alarm stations?			

OTHER PHYSICAL SAFEGUARDS

	Yes	*Risk Is Acceptable	*Corrective Action
1. Are the building and equipment correctly grounded for protection from damage by lightning?			
2. Will the computer room ceiling protect the room from flood water on the floor above?			
3. Are overhead water and steam pipes eliminated (except for sprinkler)?			
Are the computers excluded from basement areas which might flood?			
4. Will the drainage system take water away from the computers?			
5. Have steps been taken to give the installation "low visibility"?			
6. Does the computer room have self-locking doors with "panic bars" on the inside?			
7. Is access to the building controlled by guards or other means?			
8. Do the computer room personnel know how to handle unauthorized intruders?			

* These 3 response columns are mutually exclusive. Columns 2 and 3 are to be completed only if column 1 is not.

	Yes	*Risk Is Acceptable	*Corrective Action
9. Is an electronic system used to detect intruders?			
10. Are food and beverages banned in the computer room or confined to a side table?			

TAPE AND DISK LIBRARY

	Yes	*Risk Is Acceptable	*Corrective Action
1. Are magnetic tapes, disk packs, and data cells stored in a closed, dust free, fire resistant, and lockable library area or cabinet?			
2. Is there one person who is responsible for administration or the Tape Library?			
3. Is there an inventory list of tapes, disk packs, and data cells?			
4. Is sensitive material identified? Stored in locked cabinets within the library? Is there also strict accountability for copies of sensitive material?			
5. Is there a secure offsite storage facility for maintaining backup copies of vital data, programs, and documentation?			

* These 3 response columns are mutually exclusive. Columns 2 and 3 are to be completed only if column 1 is not.

CONTINGENCY PLANNING

	Yes	*Risk Is Acceptable	*Corrective Action
1. Does the installation have a formal written contingency plan?			
2. Has the plan been tested by drills, exercises, or third-party reviews?			
3. Have such tests been performed within the current year?			
4. At the minimum, do the plans provide that a current copy of all data essential to continue your program function be stored offsite?			
5. Are copies of documentation stored offsite?			
6. Are backup copies of documentation reviewed periodically to assure applicability?			
7. Have all critical jobs been identified and prioritized?			
8. Do alternative sources of processing have adequate capacity for critical jobs?			

Signed: ______________________________ Date: __________
Installation Manager or other responsible authority

* These 3 response columns are mutually exclusive. Columns 2 and 3 are to be completed only if column 1 is not.

CHAPTER 6. LOSS EXPOSURE ANALYSIS

1. Introduction. The determination of the magnitude of risk to the installation will be used as a guide in identifying areas requiring additional protection. This process is used to estimate annual losses of each asset based on the annual occurrence rate of each identified threat. The results of this analysis will be used in the cost/benefit analysis (see Chapter 8 of this handbook). If the results of the analysis seem disproportionate or improbable, it may be that previous assumptions are invalid and should be reconsidered.

2. Corequisites.

A. A calculator.

B. The Annual Loss Expectancy Worksheet (Illustration 1).

C. The Summary Risk Analysis Worksheet (Illustration 2).

D. The completed Assets/Threats Matrix (Illustration 3, Chapter 5).

E. The completed Threats Analysis Worksheets (Illustrations 1 and 2, Chapter 5).

F. The completed Assets Analysis Worksheet (Illustration 1, Chapter 3).

3. Annual Loss Exposure. For this task refer to the completed Assets/Threats Matrix, Threats Analysis Worksheets, and Assets Analysis Worksheets for information required in filling out the Annual Loss Expectancy Worksheet. The following instructions are provided for filling out this worksheet.

A. Threat and Probability Column.

(1) Use a separate worksheet for each individual minor and major threat identified on the Threats Analysis Worksheet. Then list each major and minor threat in this column.

(2) Convert the corresponding frequency of each threat on the Threats Analysis Worksheets to an annual frequency according to the following table. Place the annual frequency for each threat, as calculated below, in parentheses on the worksheet.

Frequency	Annual Frequency
1/day	360.0
1/month	12.0
1/year	1.0
1/2 years	.50
1/3 years	.33
1/4 years	.25
1/5 years	.20
1/10 years	.10
1/20 years	.05

(3) Now list each key application identified on the Applications Analysis Worksheet under EACH threat. Follow with each asset identified on the Asset Analysis Worksheet.

B. Cost Per Occurrence Column.

(1) Ignore this column for all key applications.

(2) For all assets, use the totals in the Asset Analysis Worksheet.

C. Annual Loss Expectancy (ALE) Column. The first three subcolumns will contain calculations based on numbers obtained from the Risk Analysis Worksheet, and therefore, only apply to key applications. The fourth subcolumn will contain calculations based on the replacement values of identified assets from the Assets Analysis Worksheet, and therefore, only applies to assets.

(1) Data Integrity (DI) Subcolumn. This figure is obtained by multiplying the annual frequency of the threat by the Data Integrity figure obtained on the Risk Analysis Worksheet corresponding to the threat type (major or minor) for the application.

(2) Data Confidentiality (DC) Subcolumn. This figure is obtained by multiplying the annual frequency of the threat by the Data Confidentiality figure obtained on the Risk Analysis Worksheet corresponding to the threat type (major or minor) for the application.

(3) Operational Reliability (OR) Subcolumn. This figure is obtained by multiplying the annual frequency of the threat by the Operational Reliability figure from the Risk Analysis Worksheet corresponding to the threat type (major or minor) for the application.

(4) Asset Integrity (AI) Subcolumn. This figure is obtained by multiplying the annual frequency of the threat by the replacement value figure from the Asset Analysis Worksheet.

D. Total ALE Column. For each application and asset, add the Annual Loss Expectancies to obtain the total ALE.

4. Summaries.

A. Risk Analysis Summary Worksheet. For this task, use the Risk Analysis Summary Worksheet. Fill out this form by listing all threats as indicated providing the numbers just calculated on the Annual Loss Expectancy Worksheet for each.

B. Rank Threats. From the Risk Analysis Summary Worksheet, Annual Loss Expectancy column, rank the threats from major to minor and highest to lowest dollar value ALE's. This will be used in Chapter 8 in establishing priorities of recommended safeguards. An example is provided below.

Threats	ALE
Intentional Release of Data	$ 550,000
Water Damage	217,606
Natural Hazard	108,813
Hardware Failure	86,720
Fire	65,301
Accidental Damage	21,680
Software Failure	21,680
Intentional Damage	21,680
A/C Failure	6,504
Unauthorized Physical Access	1,084

MINERALS MANAGEMENT SERVICE
ANNUAL LOSS EXPECTANCY WORKSHEET

Organization: MMS
ADP Installation: Alaska
Date: 12-5-85

DI: Data Integrity
DC: Data Confidentiality
OR: Operational Reliability
AI: Asset Integrity
* : Replacement Value of Asset

Threat and Probability	Cost Per Occurrence*	Annual Loss Expectancy				Total ALE
		DI	DC	OR	AI	
Software Failure (1/yr,1)						
GNG		1,440		1,920		3,360
Montcar		320		480		800
Presto		320		480		800
OIS		880		1,120		2,000
Postsale		320		3,200		3,520
CLASS		640		8,000		8,640
OCSIS		640		1,920		2,560
Total		4,560		17,120		21,680
Unauthorized Physical Access (1/10 yrs, .10)						
GNG		144		192		336
Montcar		32		48		80
Presto		32		48		80
OIS		88		112		200
Postsale		32		320		352
CLASS		64		800		864
OCSIS		64		192		256
Total		456		1,712		2,168

MINERALS MANAGEMENT SERVICE
RISK ANALYSIS SUMMARY WORKSHEET

Organization: MMS

ADP Installation: Alaska

Date: 12/5/85

DI:	Data Integrity
DC:	Data Confidentiality
OR:	Operational Reliability
AI:	Asset Integrity
ALE:	Annual Loss Expectancy

Threat	DI	DC	OR	AI	ALE
MAJOR					
Fire	9,488		8,446	47,367	65,301
Natural Hazard	15,808		14,060	78,945	108,813
Internal Water	31,604		28,112	157,890	217,606
Intentional Release of Data		550,000			550,000
Total Major	56,900	550,000	50,618	284,202	941,720
MINOR					
A/C Failure	1,368		5,136		6,504
Hardware Failure	18,240		68,480		86,720
Software Failure	4,560		17,120		21,680
Unauthorized Physical Access	456		1,712		2,168
Accidental Damage	4,560		17,120		21,680
Unauthorized Access	228		856		1,084
Intentional Damage	4,560		17,120		21,680
Total Minor	33,972		27,544		161,516
Total ALE	90,872	550,000	178,162	284,202	1,103,236

CHAPTER 7. SAFEGUARD ANALYSIS

1. Introduction. A wide range of safeguards is available to counter the effects of all threats and vulnerabilities identified in Chapter 5 of this handbook. The purpose of this chapter of the report is to determine appropriate countermeasures for threats and vulnerabilities previously identified. These safeguards will be analyzed for cost effectiveness and recommended if appropriate (see Chapter 8 of this handbook).

2. Safeguard Categories. Consider the following categories of countermeasures and determine those appropriate to identified threats and vulnerabilities.

A. Administrative or procedural safeguards, when used with physical controls, can produce the highest degree of security for the lowest cost of all forms of protection. Some examples of administrative safeguards are:

(1) ADP access authorizations for contractor and Government computer users.

(2) Offsite storage for data and program files.

(3) Configuration management standards for system/program development, modification, and testing.

(4) Preparation and testing of Continuity of Operations Plans (COOP's).

(5) Physical control of computer outputs (i.e., keep outputs in lockable bins, mark sensitive outputs, and require users to sign for outputs).

(6) Restrict inputs by both specifying physical and programmed restrictions on terminals processing critical data.

(7) Review user access privilege and transaction authority to ensure authorizations are necessary and consistent with current contractor and Government staffing.

(8) Define correction procedures to be used for input errors, i.e., types and classes of errors, correction procedures for error processing, authorization and verification procedures, and logging procedures for corrected transactions.

(9) Logging procedures for visitors, computer operations, computer printouts, and restricted access areas.

(10) Separation of duties for critical/key positions and careful restriction of duties between programmers, operators, and users.

(11) Termination procedures for ADP users and personnel which include turnover of passwords, documentation, manuals; cancellation of passwords, keys; and briefing on the employee's continuing legal responsibility with a signed debriefing statement by the employee.

B. Technical safeguards consist of those oriented towards controlling the technical aspects of the computer environment for both software and hardware. Some examples are:

(1) Employing configuration management techniques to control the development and evolution of systems. These can encompass documentation, software quality assurance, systems life cycle, and computer librarian functions.

(2) Use of access control software (RACF, ACF2, SECURE, SAC, and TOP SECRET) for additional control of access to sensitive data and programs.

(3) Limiting system log-on attempts from remote terminal devices.

(4) Lockout processes by developing controls to restrict critical transactions and terminals to specific time periods.

(5) Controlling dialup mode by using automatic dialback for terminal authentication, maintaining the confidentiality of dialup telephone numbers, and changing dialup phone numbers at regular intervals.

C. Physical safeguard examples consist of the following:

(1) Electronic access control systems used to monitor physical access to all restricted areas.

(2) Intrusion detection systems used to monitor unauthorized entry into restricted areas.

(3) Environmental control, detection and alarm systems used to monitor fire, air conditioning, water, emergency power, uninterruptible power supply (UPS), and humidity.

(4) Waterproof covers to prevent damage from overhead flooding or sprinkler discharge.

(5) Emergency action training for fire evacuation/ suppression, power failures, natural disasters, and emergency first aid.

(6) Operations procedures including media library procedures, backup/recovery of computer operations, computer startup, maintenance, and file handling.

CHAPTER 8. COST BENEFIT ANALYSIS AND SAFEGUARD RECOMMENDATIONS

1. Introduction. This final phase of the ADP risk analysis will aid in the determination of remedial measures by demonstrating the reduction in expected annual losses should selected countermeasures be implemented.

2. Corequisites.

A. Blank Net Benefit Calculation Worksheets (Illustration 1).

B. List of safeguards identified in Chapter 7.

C. Completed Assets/Threats Matrix (Illustration 3, Chapter 5).

D. Completed Threats Analysis Worksheets (Illustrations 1 and 2, Chapter 5).

E. Completed ADP Security--Risk Assessment Questionnaire (Appendix 1, Chapter 5).

3. Recommend Appropriate Safeguards. Based on determinations made in previous chapters, recommend appropriate safeguards to counter the effects of identified threats and vulnerabilities. Consider any long-term benefits or multiple effects benefits.

4. Determine Safeguard Costs. Determine implementation costs of safeguards identified in Chapter 7 of this handbook. These costs should be limited to one-time implementation and annual maintenance costs and can be obtained from subject-matter experts.

5. Complete the Net Benefit Worksheet. An example is provided in Illustration 1.

A. Threats/Vulnerabilities. This information is available from Chapter 5 of this handbook. Use a separate worksheet for each threat/vulnerability as it corresponds to each asset.

B. Asset. This information is available from the Assets/ Threats Matrix.

C. Additional Countermeasures. Refer to Chapter 7 of this handbook as necessary to fill out this part.

(1) If the same countermeasure has been recommended for more than one threat/vulnerability combination, list it only once.

(2) If two or more countermeasures have been recommended for the same threat/vulnerability, they must be included in the analysis to provide a comparison, if necessary.

D. Threat Occurrence Rate. This information was calculated earlier in the Threats Analysis Worksheet as the threat frequency.

E. Percentage Reduction in Threat Rate. This number is the estimated percentage reduction in the threat rate upon implementation of the recommended safeguard. For example, if water damage from the area fire extinguishing system were expected to occur once every 10 years and the recommended countermeasure were to purchase plastic covers for the ADP equipment, then such damage might only occur once in 15 years, for a 50 percent reduction in the threat rate.

F. Annualized Monetary Loss Expectancy. Refer to the Risk Analysis Summary Worksheets for this information.

G. Annual Loss Reduction. Multiply Part E with F.

H. Annualized Cost of Countermeasure. Divide the cost of the countermeasure by its life expectancy.

I. Total Net Benefit. Subtract Part H from Part G.

6. Rank Safeguards.

A. Arrange the completed Net Benefit Worksheets according to Part I.

B. Summarize recommended safeguards. Include discussion of basis for recommendation and net benefits if implemented. A simplified example follows.

Safeguard Number 1. Increase the frequency of the backup cycle from quarterly to weekly. This would involve mailing seven magnetic tapes to the Pacific OCS Region on a weekly basis. Net benefit = $69,216.

Safeguard Number 2. Procure waterproof plastic covers for computer equipment. Net benefit = $43,421.

C. Prepare a summary table of the cost/benefit analysis of all recommended safeguards. An example follows.

Safeguard	Total Cost	Life Expectancy	Annualized Cost
Number 1	N/A	N/A	$7,680
Number 2	$1,000	10 years	$ 100

MINERALS MANAGEMENT SERVICE
WORKSHEET NET BENEFIT CALCULATION

A Threat/Vulnerability Internal Water Damage

B Asset Data, Operations, Physical Assets

C Additional countermeasure Waterproof Plastic Covers for Equipment

D Threat occurrence rate (1/10 years, .10)

E Percentage reduction in threat rate 20%

F Annualized monetary loss expectancy or annualized nonmonetary impact $217,606

G Annual loss reduction:

F x E = $43,521

*H Annualized cost of countermeasure $100

J Total net benefit (G - H) = $43,421

* Total cost $1,000
Useful life 10 years

3D140248 3VBS